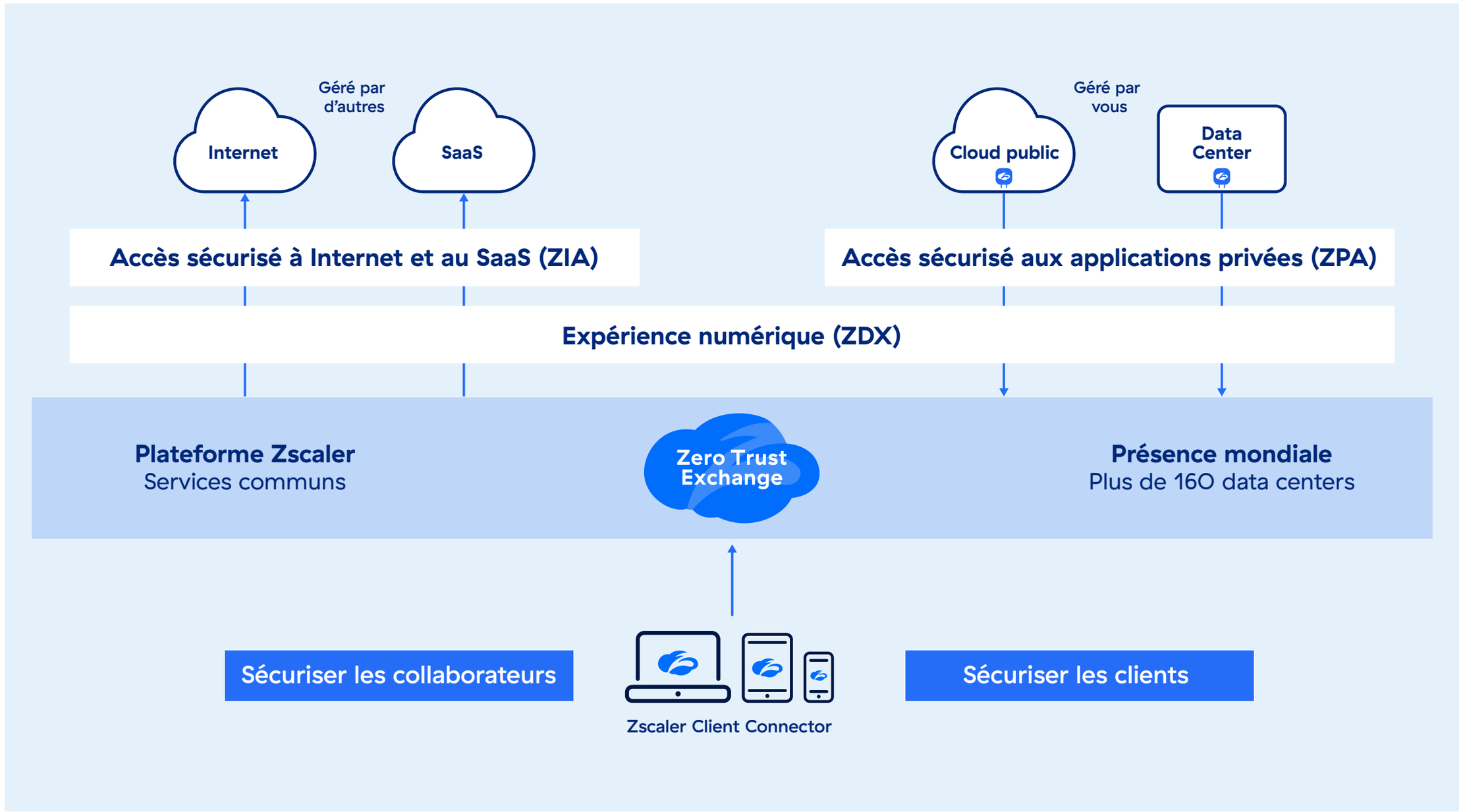
Zscaler Client Connector

Accès rapide, sécurisé et fiable à n'importe quelle destination, depuis n'importe quel emplacement ou appareil.

FICHE TECHNIQUE

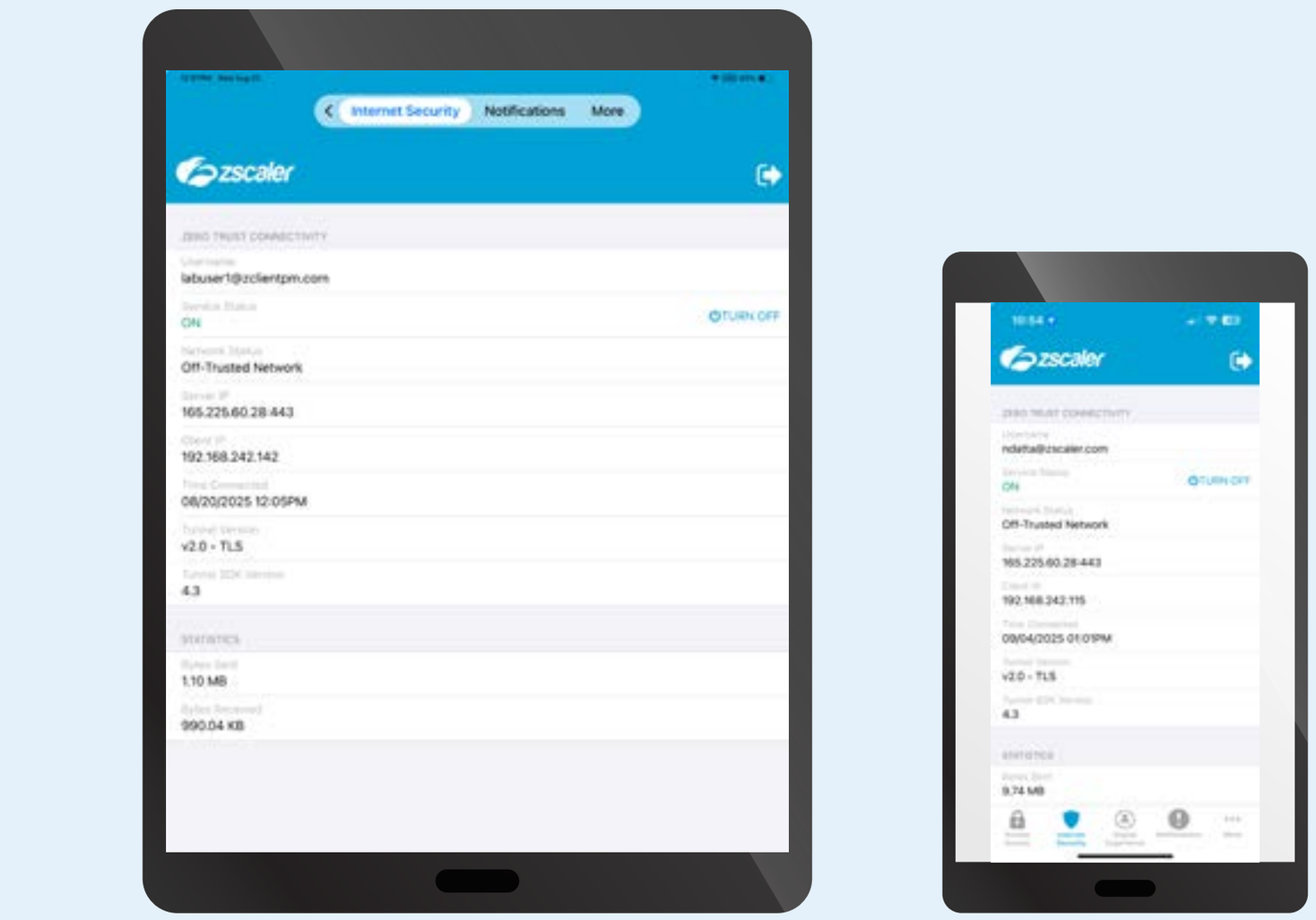


De nos jours, les employés travaillent de manière radicalement différente. Ils peuvent désormais utiliser une grande variété d'appareils, travailler depuis n'importe où, et accéder à des applications cloud et à d'autres destinations dans le monde. Ce nouveau personnel hybride exige un accès rapide et fluide aux ressources informatiques, mais cela ne doit pas se faire au prix d'une exposition dangereuse des données. Par conséquent, toute entreprise qui veut réussir doit sécuriser des terminaux distribués à l'échelle mondiale tout en garantissant des expériences utilisateur productives. Pour ce faire, de très nombreuses équipes informatiques se tournent vers Zscaler et son aagent de point de terminaison, Client Connector.

Par le passé, lorsque les utilisateurs et les applications se trouvaient au bureau, il était logique de s'appuyer sur des solutions de sécurité et de connectivité centrées sur le réseau. Mais aujourd'hui, les employés hors site accèdent à des applications hors site via des réseaux que les équipes informatiques ne contrôlent pas. Backhauler ce trafic vers le data center pour le sécuriser ajoute une latence qui perturbe la productivité. Plus important encore, le backhauling augmente les risques en connectant les utilisateurs au réseau de l'entreprise, leur permettant d'abuser de permissions excessives et de se déplacer latéralement à travers les ressources connectées au réseau, sans compter qu'il élargit la surface d'attaque et engendre d'autres failles de sécurité majeures.

L’architecture Zero Trust est la solution à ces problèmes. Zscaler la fournit en tant que service à partir de Zero Trust Exchange, la plus grande plateforme de sécurité cloud au monde, qui agit comme un standard intelligent pour fournir des communications Zero Trust any-to-any en utilisant des politiques d’entreprise et non des réseaux. Zero Trust Exchange fournit un accès sur la base du moindre privilège directement aux ressources informatiques en fonction du contexte et non de l’adresse IP de l’utilisateur, et ce à la périphérie à partir de plus de 160 points de présence dans le monde. En d’autres termes, les équipes informatiques peuvent mettre fin aux menaces et aux pertes de données tout en offrant aux utilisateurs des expériences numériques exceptionnelles sur n’importe quel appareil, n’importe où.

Zscaler Client Connector joue un rôle central dans la prestation de communications any-to-any Zero Trust. Il s’agit de l’agent de terminal léger, mais polyvalent de Zscaler, qui facilite un accès performant et le moins privilégié directement à Internet et aux ressources informatiques pour les utilisateurs, où qu’ils se trouvent. Il propose une multitude d’autres fonctionnalités qui améliorent encore la sécurité et la connectivité, et éliminent les produits ponctuels et leurs agents dédiés.



© 2025 Zscaler, Inc. Tous droits réservés.

Avantages de Zscaler Client Connector

Les avantages de Client Connector peuvent plus ou moins être regroupés en sept catégories. Pour plus de détails, veuillez consulter le tableau à la fin de cette fiche technique.

Communications Zero Trust vers n'importe quelle destination
Les entreprises n'ont plus besoin de solutions distinctes avec des agents distincts pour sécuriser l'accès à différentes destinations. Client Connector offre un accès Zero Trust avec le minimum de privilèges à toutes les destinations, y compris le web, les solutions SaaS et les applications privées. Ceci s'inscrit dans la vision de Gartner dédiée au SSE et au SASE et garantit que les appareils ne sont pas ralentis par la prolifération d'agents.

Communications Zero Trust pour tous les appareils
Outre l'accès à toutes les destinations, les entreprises doivent également sécuriser l'accès sur tous les appareils. En effet, les employés utilisent désormais des ordinateurs de bureau, ordinateurs portables, tablettes et smartphones, dotés de différents systèmes d'exploitation. Heureusement, Client Connector peut sécuriser n'importe quel appareil et garantir la sécurité et la productivité de vos employés.

Sécurité intelligente et contextuelle
L'identité seule ne suffit pas à gérer l'accès aux ressources informatiques (les identités peuvent être volées, et même des utilisateurs légitimes peuvent nuire à leurs employeurs par inadvertance). Les entreprises doivent gérer l'accès en fonction du contexte et des risques. Client Connector fournit des informations concernant la sécurité des appareils, pour un contrôle d'accès intelligent et adaptatif.

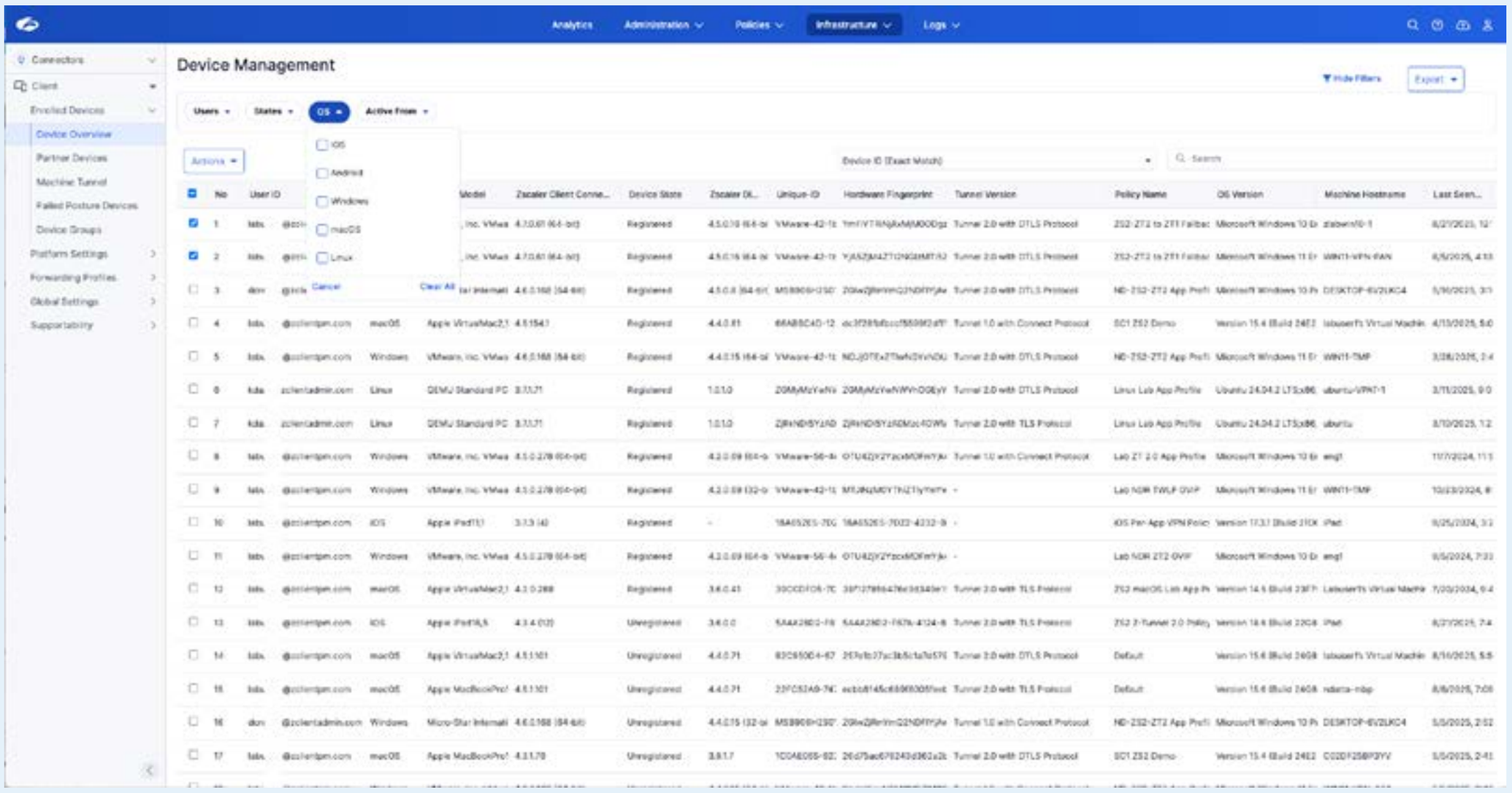
Protection des données sur les appareils des utilisateurs finaux
Dans le cadre de l'offre complète de sécurité des données de Zscaler, qui sécurise tout canal de fuite, Client Connector propose une solution DLP pour les terminaux. Elle permet aux entreprises de sécuriser le stockage amovible, les partages réseau, la synchronisation du stockage cloud personnel et l'impression sur les terminaux sans recourir à un quelconque produit ponctuel qui doit être géré séparément.

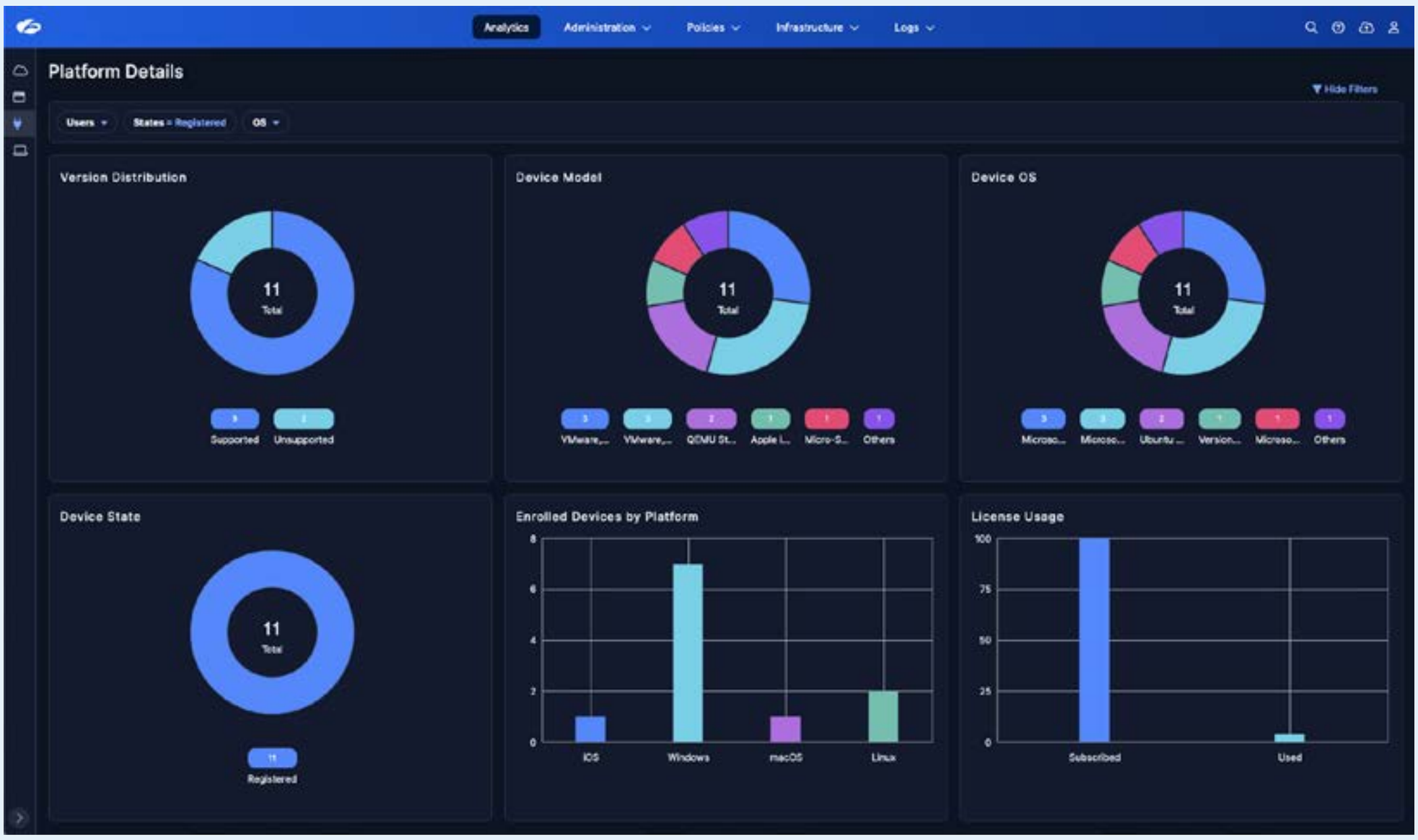
Détection des menaces cachées dans votre environnement
Des adversaires furtifs se dissimulent souvent dans l'environnement des entreprises pour préparer des stratagèmes malveillants. Client Connector s'appuie sur une technologie de tromperie qui utilise des leurres réalistes de signets d'applications, de cookies, de sessions et de mots de passe pour attirer ces hackers. Dès que ceux-ci accèdent à un de ces leurres, il génère des alertes hautement fiables.

Expérience utilisateur et productivité supérieures
Contrairement aux outils traditionnels qui renvoient le trafic, Client Connector oriente le trafic vers sa destination par le chemin le plus court. Il offre également à Zscaler Digital Experience (ZDX) une visibilité sur les événements et l'état des appareils, ce qui permet aux administrateurs de disposer d'une vue d'ensemble de la connexion de l'utilisateur, d'accélérer la résolution des problèmes d'expérience utilisateur et d'améliorer la productivité des utilisateurs et des administrateurs.

Gestion simplifiée basée sur le cloud
La gestion de Client Connector avec l'interface utilisateur unifiée de Zscaler, Experience Center, optimise l'excellence opérationnelle. Elle permet une gestion continue des politiques et du cycle de vie pour gérer les transferts, la sécurité, les mises à niveau et les rollback, grâce à des tableaux de bord et des rapports intégrés. Les administrateurs peuvent également automatiser les tâches via OneAPI, une API unique pour l'ensemble de la plateforme Zscaler.

© 2025 Zscaler, Inc. Tous droits réservés.





© 2025 Zscaler, Inc. Tous droits réservés.

MODULES DE ZSCALER CLIENT CONNECTOR

Zscaler Internet Access	S'appuyant sur une décennie de leadership dans le Magic Quadrant dédié au Secure Web Gateway (SWG), ZIA est la solution Zscaler qui sécurise l'accès à Internet tout en appliquant diverses fonctionnalités de protection granulaire contre les menaces.
Zscaler Private Access	Zscaler Private Access offre des communications Zero Trust homogènes pour tous les utilisateurs accédant à n'importe quelle application privée, avec une segmentation utilisateur–application optimisée par IA et des politiques adaptées au contexte qui contribuent à réduire les risques.
Zscaler Digital Experience	Zscaler Digital Experience fournit une visibilité de bout en bout sur les expériences utilisateur et permet une détection, un dépannage et une résolution rapides des problèmes de performances.
Zscaler Endpoint DLP	Zscaler Endpoint Data Loss Prevention (DLP) est une composante de la solution complète Zscaler Data Security. Elle fournit la visibilité et le contrôle dont vous avez besoin sur les données présentes sur les appareils tout en réduisant le coût et la complexité de la sécurité des données.
Zscaler Deception	Zscaler Deception déploie des leurres réalistes dans tout votre environnement informatique et génère des alertes très précises qui permettent de détecter et de neutraliser plus rapidement les menaces.

CARACTÉRISTIQUES ET DÉTAILS DE CLIENT CONNECTOR

Prise en charge complète du système d'exploitation	**Ordinateurs de bureau et clients légers :** • Microsoft Windows 11 et Windows 10 sur x64 et ARM64 • Apple macOS Tahoe (26), Sequoia (15) et Sonoma (14) sur Intel et Apple Silicon • Postes de travail Linux (RHEL, CentOS, Fedora, Ubuntu, Debian, openSUSE, Arch Linux, Maya OS) • Google Android sur ChromeOS • Systèmes d'exploitation eLux et IGEL **Mobile :** • Apple iOS 17, 18 et 26 • Google Android 10, 11, 12, 13, 14, 15 et 16
Supporte VDI mono–utilisateur et multi–utilisateur	• Windows 365 Cloud PC, Azure Virtual Desktop • AWS Workspaces • Applications et bureaux virtuels Citrix • Omnissa Horizon et Horizon Cloud Environnements VDI multisessions pris en charge avec Client Connector pour VDI

© 2025 Zscaler, Inc. Tous droits réservés.

Prise en charge étendue des types de trafic	• Tous les ports et protocoles (Z-Tunnel 2.0) • Trafic Web uniquement (Z-Tunnel 1.0) • Trafic client à client • Trafic serveur vers client
Transport par tunnel	DTLS 1.2, TLS 1.2 et HTTP CONNECT
Chiffrement	• Authentification TLS mutuelle • Épinglage SSL pour la connectivité du canal de contrôle • Conformité FIPS140
Sélection optimale des DC	Sélection automatique Basée sur des politiques : Géolocalisation, DC préférés, latence et destination du trafic
Prise en charge du protocole de couche 3	IPv4 et IPv6
Méthodes de connectivité flexibles	• Initié par l'utilisateur • À la demande • Prise en charge de la pré-connexion avec les tunnels de machines • Toujours activé • Prise en charge du profil VPN d'entreprise ou du profil VPN par application sur iOS • Prise en charge du double tunnel (profil VPN d'entreprise et VPN par application) sur iOS • Prise en charge du profil de travail pour Android
Options de déploiement et de cycle de vie	• Déploiement à l'aide de MDM et UEM comme Intune, Workspace ONE, JAMF Pro, MobileIron, MaaS360, SCCM et d'autres solutions • Déploiement à l'aide de Microsoft GPO dans Active Directory (AD) • Déploiements manuels à l'aide de téléchargements directs depuis Zscaler • Mises à jour des versions gérées dans le cloud et prise en charge du rollback • Distribution homogène de certificats d'autorité de certification racine de confiance pour l'inspection SSL • Gestion des politiques et des appareils basée sur les API
Provisionnement des utilisateurs selon les normes de l'industrie	• Système de gestion des identités inter-domaines (SCIM) • Provisionnement « Just in Time » basé sur SAML 2.0 • Provisionnement « Just in Time » pour l'accès d'urgence des utilisateurs • Provisionnement automatique des appareils basé sur une clé machine • Provisionnement automatique utilisateur/appareil basé sur un jeton • Provisionnement de certificats basé sur SCEP* • Synchronisation du serveur d'annuaire Microsoft AD ou LDAP • Ajout manuel ou téléchargement en masse d'utilisateurs vers la base de données d'utilisateurs hébergée

© 2025 Zscaler, Inc. Tous droits réservés.

Options d'authentification prises en charge	• SAML 2.0 • Kerberos • Certificats et cartes à puce • Authentification multifacteur (MFA). • Prise en charge des jetons matériels compatibles FIDO2 • Authentification de l'appareil basée sur une clé machine pour la prise en charge de la pré-connexion • Authentification utilisateur/appareil basé sur un jeton • Mots de passe • Prise en charge de l'authentification renforcée • Authentification basée sur le navigateur
Authentification unique	• SSO fluide pour Windows • SSO Kerberos • Plug-in Microsoft Enterprise SSO pour macOS et iOS • Prise en charge du framework Apple Enterprise SSO • Prise en charge de l'extension OKTA SSO
Restrictions d'utilisation basées sur des politiques	• Support anti-falsification • Restrictions OTP et mot de passe pour contrôler la déconnexion de l'utilisateur, la sortie du client et les restrictions d'arrêt du service
Langues prises en charge	anglais, français
Notifications aux utilisateurs finaux	**Prise en charge des notificationsde bureau et de système d'exploitation pour :** • Notifications de politique d'utilisation acceptable • État du service • Mises à jour logicielles • Authentification et réauthentifications périodiques • Événements de sécurité des données inline • Notifications et flux de travail DLP des terminaux • Notifications d'événements liés à la politique d'accès à Internet et aux applications privées • Protection contre les menaces avancées • Notifications de sécurité Zscaler Zero Trust Firewall, IPS et DNS • Prise en charge des notifications Zscaler Digital Experience Co-pilot
Outils de dépannage intégrés	• Récupération automatique des journaux chiffrés • Exportations manuelles des journaux • Prise en charge de la capture automatique et manuelle des paquets • Prise en charge de l'automatisation pour la surveillance et la gestion des services

© 2025 Zscaler, Inc. Tous droits réservés.

Prise en charge étendue de la posture	• Chemin du fichier • Clé et valeur de registre • Certificat de confiance • Certificat client avec CRL • Certificat client validé par le serveur • État du pare-feu • Chiffrement complet du disque • Statut de jonction de domaine AD • Statut de jonction du domaine Entra • Contrôles de processus • Détection en temps réel de Carbon Black • IP de sortie du client • Détection Microsoft Defender en temps réel • Détection CrowdStrike en temps réel • Score de CrowdStrike ZTA Device OS • Score de CrowdStrike ZTA Sensor • Détection antivirus • Vérifications de la version du système d'exploitation • Détection d'agent JAMF • Niveau de risque JAMF • Modification non autorisée • Variable de propriété • Version de Zscaler Client Connector
Autres capacités	• Prise en charge de la reprise après sinistre et de la continuité d'activité • Gestion de portail captif intégré avec verrouillage réseau en option • Gestion du pare-feu des terminaux Client Connector avec blocage du réseau local • Prise en charge de la mise en quarantaine des appareils • Détection et commutation automatisées de réseaux de confiance • Prise en charge de l'environnement sans route par défaut (NDR)

À propos de Zscaler

Zscaler (NASDAQ : ZS) accélère la transformation numérique pour améliorer l'agilité, l'efficacité, la résilience et la sécurité de ses clients. La plateforme Zscaler Zero Trust Exchange™ protège des milliers de clients contre les cyberattaques et la perte de données, en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quel que soit leur emplacement. Adossé à plus de 160 data centers dans le monde, Zero Trust Exchange™, basé sur SSE, constitue la plus vaste plateforme de sécurité cloud inline au monde. Pour en savoir plus, rendez-vous sur **zscaler.com/fr** ou suivez-nous sur X (ex-Twitter) **@zscaler**.

© 2025 Zscaler, Inc. Tous droits réservés. Zscaler™ et les autres marques commerciales répertoriées sur **zscaler.com/fr/legal/trademarks** sont soit 1) des marques déposées ou marques de service, soit 2) des marques commerciales ou marques de service de Zscaler, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques commerciales appartiennent à leurs propriétaires respectifs.

+1 408 533 0288 **Zscaler, Inc. (siège) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/fr**

zscaler™

Zero Trust Everywhere